## CLAIMS

1. A method of providing automated document retention for electronic documents, said method comprising:

obtaining an electronic document;

assigning a document retention policy to the electronic document, the document retention policy being based on a future event that is unscheduled; and

cryptographically imposing the document retention policy on the electronic document.

2. A method as recited in claim 1, wherein said method further comprises:

subsequently determining whether the future event has occurred; and

cryptographically preventing access to the electronic document in accordance with the document retention policy based on the occurrence of the future event.

3. A method as recited in claim 2, wherein said determining is periodically performed.

4. A method as recited in claim 2, wherein said determining is performed by interacting with a network accessible resource.

5. A method as recited in claim 2, wherein said determining is performed by interacting with a web accessible resource.

6. A method as recited in claim 5, wherein said determining comprises:

supplying a future event description of the future event to the web accessible resource; and

determining, at the web accessible resource, whether the future event has occurred.

7. A method as recited in claim 6, wherein said supplying is achieved by a universal resource locator associated with the future event description.

8. A method as recited in claim 5, wherein said determining comprises:

supplying the future event description to a contract management system; and

determining, at the contract management system, whether the future event has occurred.

9. A method as recited in claim 1,

wherein said imposing operates to utilize a cryptographic key to impose the document retention policy, and

wherein the document retention policy specifies a document retention period based on the future event.

10. A method as recited in claim 9, wherein the document retention policy specifies a document retention period that expires a predetermined period of time after the occurrence of the future event.

11. A method as recited in claim 9, wherein said method further comprises:

determining whether the document retention period has expired; and

deactivating the cryptographic key when said determining determines that the document retention period has expired, thereby preventing further access to the electronic document.

12. A method as recited in claim 11, wherein said method further comprises:

permitting said deactivating to be overridden so that the electronic document can remain accessible even after the document retention period.

13. A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data;

obtaining a document key;

encrypting the data portion of the electronic document using the document key to produce an encrypted data portion;

obtaining a retention access key, the retention access key being used to enforce a document retention policy on the electronic document;

encrypting the document key using the retention access key to produce an encrypted document key;

forming a secured electronic document from at least the encrypted data portion and the encrypted document key; and

storing the secured electronic document.

14. A method as recited in claim 13, wherein the retention access key is a public retention access key.

15. A method as recited in claim 13, wherein the document retention policy is dependent on a future event that is presently unscheduled, and the retention access key is used to enforce the document retention policy on the electronic document.

16. A method as recited in claim 15, wherein the retention access key is subsequently available from a remote key store only so long as a document retention period of the document retention policy has not been exceeded.

17. A method as recited in claim 16, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

18. A method as recited in claim 17, wherein said method further comprises:

extending the predetermined period of time after the occurrence of the future event.

19. A method as recited in claim 15, wherein said method is performed on a client machine that operatively receives the retention access key from the remote key store over a network.

20. A method for accessing a secured electronic document by a requestor, the secured electronic document having at least a header portion and a data portion, said method comprising:

obtaining a retention access key, the retention access key being used to enforce a document retention policy on the electronic document;

obtaining an encrypted document key from the header portion of the secured electronic document;

decrypting the encrypted document key using the retention access key to produce a document key;

decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion; and

supplying the data portion to the requestor.

21. A method as recited in claim 20, wherein the retention access key is identified by an indicator within a header portion of the secured electronic document.

22. A method as recited in claim 20, wherein the retention access key is a private retention access key.

23. A method as recited in claim 20, wherein, if permitted, said obtaining obtains the retention access key being obtained from a server.

24. A method as recited in claim 20, wherein the document retention policy is dependent on a future event that is presently unscheduled, and the retention access key is used to enforce the document retention policy on the electronic document.

25. A method as recited in claim 20, wherein the retention access key is available only so long as a document retention period of the document retention policy has not been exceeded.

26. A method as recited in claim 25, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

27. A method as recited in claim 20, wherein the retention access key is available from a remote key store only so long as a document retention period of the document retention policy has not been exceeded.

28. A method as recited in claim 20, wherein the retention access key is available only so long as a document retention period of the document retention policy has not been exceeded, the document retention period can be extended to permit extended access to the electronic document.

29. A method for distributing cryptographic keys used in a file security system, said method comprising:

receiving a request for a document retention key that is necessary to gain access to a cryptographically secured electronic document;

identifying a document retention period associated with the document retention key, the document retention period being dependent on a future event that was unscheduled when the document retention period was associated with the electronic document;

determining whether the document retention period associated with the document retention key has been exceeded; and

refusing to distribute the document retention key in response to the request when said determining indicates that the document retention period for the electronic document has been exceeded.

30. A method as recited in claim 29, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

31. A method as recited in claim 29, wherein said method is performed at a server, and wherein the request for the document retention key is from a client module that is connectable to the server via a network.

32. A method as recited in claim 29, wherein the document retention period can be extended to permit extended access to the electronic document.

33. A file security system for restricting access to electronic files, said file security system comprising:

a key store that stores a plurality of cryptographic key pairs, each of the cryptographic key pairs including a public key and a private key, at least one of the

cryptographic key pairs pertaining to a retention policy, the retention policy being dependent on a future event; and

an access manager operatively connected to said key store, said access manager determines whether the private key of the at least one of the cryptographic key pairs pertaining to the retention policy is permitted to be provided to a requestor based on whether the future event has occurred,

wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the retention policy to access a secured electronic file, and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy, and at the time the electronic file was so secured, the future event was unscheduled.

34. A file security system as recited in claim 33, wherein said access manager prevents the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from being provided to the requestor after a predetermined retention period following the occurrence of the future event.

35. A file security system as recited in claim 33, wherein the requestor is a client module that operatively connects to said access manager over a network.

36. A file security system as recited in claim 33, wherein said file security system further comprises:

at least one client module, said client module assisting a user in selecting the retention policy, and said client module securing the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy so as to cryptographically impose the retention policy.

37. A file security system as recited in claim 33, wherein said file security system further comprises:

at least one client module, said client module assisting with unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertains to the retention policy from said key store if permitted by said access manager, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertains to the retention policy.

38. A computer readable medium including at least computer program code for providing automated data retention for electronic data, said computer readable medium comprising:

computer program code for obtaining electronic data;

computer program code for assigning a data retention policy to the electronic data, the data retention policy being based on a future event that is unscheduled; and

computer program code for cryptographically imposing the data retention policy to the electronic data.

39. A computer readable medium as recited in claim 38, wherein said computer readable medium further comprises:

computer program code for subsequently determining whether the future event has occurred; and

computer program code for cryptographically preventing access to the electronic data in accordance with the data retention policy based on the occurrence of the future event.

40. A computer readable medium as recited in claim 39, wherein the electronic data is an electronic file.

41. A computer readable medium as recited in claim 39, wherein the electronic data is an electronic document.

42. A computer readable medium as recited in claim 38,

wherein said computer program code for imposing operates to utilize a cryptographic key to impose the data retention policy, and

wherein the data retention policy specifies a data retention period based on the future event.

43. A computer readable medium as recited in claim 42,

wherein the data retention policy specifies a data retention period that expires a predetermined period of time after the occurrence of the future event, and

wherein said computer readable medium further comprises:

computer program code for determining whether the data retention period has expired; and

computer program code for deactivating the cryptographic key when it is determined that the data retention period has expired, thereby preventing further access to the electronic data.

44. A computer readable medium as recited in claim 43, wherein said computer readable medium further comprises:

computer program code for permitting said computer program code for deactivating to be overridden so that the electronic data can remain accessible even after the data retention period.